



April 13, 2023

Laurie E. Locascio
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Dr, Gaithersburg, MD 20899

Re: Security Industry Association Comments on draft NIST 800-63-4 (Digital Identity Guidelines)

Dear Under Secretary Locascio:

SIA is a nonprofit trade association representing more than 1,300 companies that provide life safety and security technology for government programs, commercial customers, and consumers throughout the United States. SIA members include the leading providers of identity management solutions and related biometric technologies, including products and services designed for government programs and applications.

Attached you will find section-by-section comments provided on behalf of SIA and its members, which includes 30 different items using the template provided by the National Institute of Standards and Technology (NIST). However, I also wanted to highlight our chief concern with draft revision 4 of NIST 800-63 (Digital Identity Guidelines).

We are concerned that in contrast with earlier drafts, the latest draft seeks to establish alternatives to the most reliable and secure methods of remote identity proofing available, which are required for IAL2 authentication in the current version of the Guidelines, based on unproven equity concerns. NIST should follow the latest science, cybersecurity expertise and available data, which indicate that for remote identity proofing there is simply no equivalent alternative to using biometric comparison with liveness and presentation attack detection for this purpose.

Facial recognition is a mature technology that is highly reliable for “1:1” image comparison and matching, reflected in ongoing NIST Facial Recognition Vendor Test Program (FRVT) program results.¹ Additionally, the most recent research from the DHS Science and Technology Directorate (S&T) shows dramatically improved results and accuracy across all skin tones.² For high-performing technologies available today, variation across demographics is a solved problem and should not be considered a barrier to providing inclusive and equitable identity proofing services. To be clear, alternative methods should be offered if users chose to opt out, but biometric comparison should be the standard.

¹ <https://pages.nist.gov/frvt/html/frvt11.html>

² <https://mdtf.org/Rally2022>

Without being biometrically bound to a verified government issued ID, there is no strong assurance that the remote user is who they say they are, for a digital enrollment or remote interaction. Setting this aside would reverse the evolution of more secure credentials and authentication methods at a time when they are most needed to address digital fraud and cyber-attacks, and despite growing adoption and public acceptance of digital identification such as mobile driver's licenses.

In addition to the comments provided, SIA and its members stand ready to provide any additional information needed as NIST continues efforts to update its Digital Identity Guidelines.

Respectfully,

A handwritten signature in black ink, appearing to read "Don Erickson", enclosed in a thin black rectangular border.

Don Erickson
Chief Executive Officer
Security Industry Association
Silver Spring, MD
www.securityindustry.org

Staff Contact: Jake Parker, jparker@securityindustry.org